

Risk-Informed Evaluation of Security Technology Insertions and Next-Generation Control System Architectures via Modeling and Simulation

Peter Sholander
Sandia National Laboratories, P.O. Box 5800, M/S 0672
Albuquerque, New Mexico 87185-0672
V: 505-844-0646, E: peshola@sandia.gov

1 Introduction

This workshop posits that the development of high integrity, high-confidence software and systems for networked sensing, monitoring, and control is crucial for the future of the Nation’s industries and critical infrastructures. However, our homeland security budget does not permit Industry or the Government to protect everything against all possible risks and adversaries. Instead Government must work with Industry (who own and operate most of the critical infrastructures) on next-generation control system architectures, and deployment strategies for new/existing security technologies, that are “risk informed” and provide cost-effective protection against the highest risk and highest consequence attacks.

2 Risk Assessment Process

Figure 1 outlines the risk assessment process. It begins with a definition of the threats. For human threats this includes their cyber/physical capabilities, funding levels, and motivation levels. However, the “threat” may also be natural events such as hurricanes and earthquakes – as evidenced by Hurricanes Katrina and Rita in 2005. The risk assessment process must next determine what “effects” those threats can cause. Those effects can be kinetic effects such as blowing up pipelines. The effects can also be cyber-based ones that degrade the confidentiality, integrity and availability of the information systems that control the critical assets in one or more coupled infrastructures. Next, the “impacts” (e.g., assets failures such as loss of power plants or pipelines) caused by those effects must be calculated or modeled. The final step shown in Figure 1 is to determine the “consequences” (e.g., loss of power to the entire Midwestern US) that can result from those impacts.

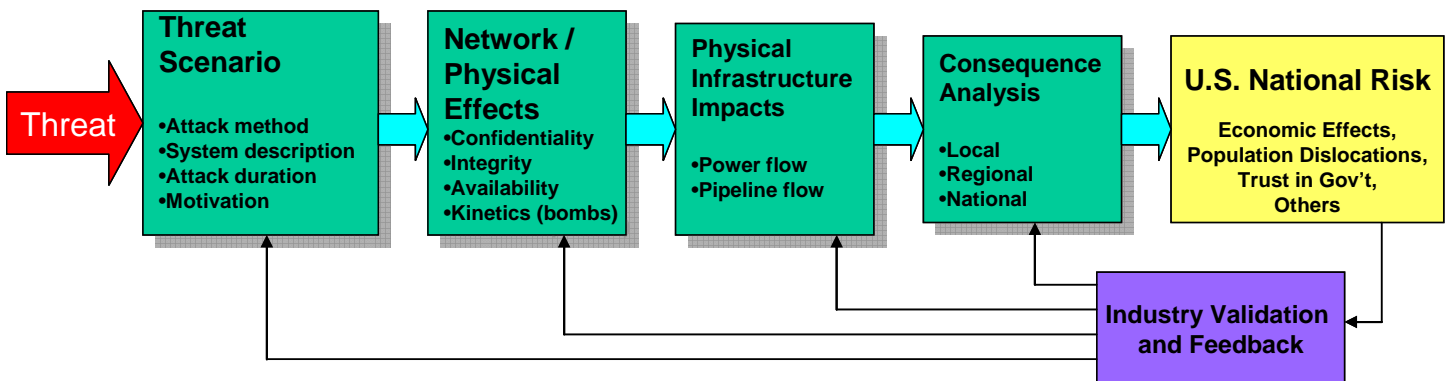


Figure 1. Risk Assessment Process

A “risk-informed” analysis must also calculate the conditional risk (to U.S. National Interests) that a given consequence will occur (based on the “evidence” that a given threat can actually cause a given impact), and then convert that conditional risk to a common unit of measure such as “willingness to pay”. This allows the relative economic merit of various control system architectures and security technologies to be evaluated. The performance of these calculations for large coupled infrastructures and a wide spectrum of threats will require an integrated set of modeling and analysis tools that does not currently exist.

3 Existing Tools and Future Work

There are existing tools for network and telecom simulation such as OPNET, QualNet and ns2. Similarly, there is a rich body of “engineering process models” and other analysis tools for water distribution, oil/gas pipelines and power generation/distribution. They include EPANET for water systems. For power generation/distribution, they include PSS/E and PowerWorld. For oil/gas pipelines, they include the Stoner Pipeline Simulator. Finally, for IP-based network research, there are test-beds such as Emulab (www.emulab.net/) and DETER (www.isi.edu/deter/) that allow for testing of effects/impacts in large-scale emulated IP networks.

Sandia and other National Labs partners (www.sandia.gov/mission/homeland/programs/critical/nisac.html) have developed agent-based models for coupled infrastructures that can be used for consequence modeling. They include:

- System dynamics modeling to quantify and evaluate the effects of infrastructures and their interdependencies on supply and demand under different conditions (e.g., time of day/year, unusual event, new regulations, incentives, market structures).
- Large-scale microeconomic simulation tools that capture complex supply chain and market dynamics of businesses in the U.S. economy for a better understanding of the impacts of vulnerabilities and disruptions on national economic security.

- A Railroad Network Analysis System that uses non-linear optimization techniques to understand their behavior under normal and disrupted situations, to examine commodity flow disruptions due to destruction of assets, and to study policy options concerning the movement of toxic chemicals by rail.
- An interdependent Energy Infrastructure Simulation System that provides a comprehensive simulation environment for interdependent energy infrastructures (focused especially on electric power and natural gas systems) based on the physics of the infrastructures, and resolved to the infrastructure component level.
- An Urban Infrastructure Suite (UIS) that is a set of seven interoperable modules that employ advanced modeling and simulation methodologies to represent urban infrastructures and populations. These modules include models for urban population mobility, epidemiology, telecommunications, transportation, and water.

The National SCADA Test Bed (which is a National Lab partnership funded by DOE/OE) is developing a “Virtual Control System Environment” (VCSE) whose goal is a combined analysis of system availability, system performance, and cyber security posture for critical infrastructures. VCSE will use a mix of real, simulated and emulated systems/software/hardware that will provide tradeoffs between cost, scalability, and accuracy. The current focus is on bulk power generation and distribution, but the goal is extensibility to coupled infrastructures and manufacturing plants. The VCSE software will leverage commercial tools (OPNET, MATLAB, HLA, ...) and internal DOE-funded research. The VCSE models will be populated based on expert opinion, facility operator documentation, vendor documentation, lab studies, and site assessments. The partitioning between real, emulated, and virtual entities in each model/experiment will be based on a particular assessment’s goals. (Note: The VCSE might be viewed as a form of “emulab” for PCS that also includes simulated entities.) A VCSE-like capability could provide both effects/impact modeling, and also “security regression testing” before security technologies are inserted into production systems.

HCSS-NEC4CPS should fund research and development efforts that link these existing tools (or similar ones) into the unified risk assessment process outlined in the previous section. Of particular interest are: a) risk assessment methodologies for blended security systems that contain both physical and cyber protections; and b) emulation techniques for PCS hardware/software.

4 Traceability to Government / Industry Needs

The integrated risk assessment and modeling tools proposed above should help address the following requirements in the *Roadmap to Secure Control Systems* (which is available at: <http://www.controlsystemsroadmap.net>):

- Measure and assess security posture for facility providers. The goal is that by 2008, 50% of asset owners and operators can perform self-assessments of their control systems using consistent criteria.
- Develop and integrate protective measures for PCS. The goal is to provide “security test harnesses” for evaluating next generation architectures and individual PCS components by 2014.

The first goal is challenging because insufficient tools and techniques currently exist to measure risk in large coupled infrastructures. In addition, the threats are hard to demonstrate and quantify to Industry. A suite of modeling tools can help an analyst determine the robustness of a system’s security posture by performing analysis on a modeled PCS and its controlled infrastructures. In most cases, an on-line operational system cannot be stressed by introducing attacks or failures to measure the system’s resilience. In addition, the cost of building large-scale test beds is prohibitive for most facility operators. As such, a modeling tool is often a practical and cost-effective solution for answering security-related questions for large systems.

With respect to the threat environment, further integration of shared telecommunications technologies into normal business operations has spawned increased levels of interconnectivity among corporate networks, control systems, other asset owners, and the outside world. This expansion of connectivity provides increased potential for cyber attacks, and new security measures are required to prevent potential attacks and mitigate the consequences of successful attacks. As such, the suite of tools outlined in this paper could help support the analysis of security measures and their impacts on system operation.

The challenge for the second goal is that security upgrades are often hard to retrofit to legacy systems, may be costly, and may degrade system performance. Security solutions that are devised for legacy systems are constrained by the limitations of existing equipment and configurations. Analyzing the interactions and behavior between emerging security solutions and existing legacy control systems is critical though for identifying any vulnerability into a proposed/upgraded control system’s security solution.

5 Author Bio

Peter Sholander received his Ph.D. from the Georgia Institute of Technology. He is currently a Principal Member of Technical Staff at Sandia National Laboratories in Albuquerque, New Mexico where he is the task lead for the VCSE tool that is being developed by the National SCADA Test Bed (NSTB). Previous employers include Bell Labs and Ford Motor Company. His interests include critical infrastructure protection, Process Control System (PCS) security, network security, wireless networking, and cargo security. He has published over 30 papers in these areas.